UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/509,872	02/03/2005	Hideyuki Suzuki	259551US6PCT	4966

22850 7590 05/29/2008
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
YOUSEFI, SHAHROUZ	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
05/29/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	**Application No.** 10/509,872	**Applicant(s)** SUZUKI, HIDEYUKI
	Examiner SHAHROUZ YOUSEFI	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 October 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *07/31/2007 and 03/05/2007*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 15-18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Data structures not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See MPEP 2106.01 and e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Akachi (US 7,069,436).

5. With respect to claim 1, Akachi discloses a first terminal that encrypts a payload of a broadcast frame and that transmits the broadcast frame (a transmitter encrypts the broadcast data, col. 1, lines 24-25); and a second terminal that receives the broadcast frame and that decodes the payload of the broadcast frame (the subscribers decode the

received encrypted signals using the private key, col. 1, lines 26-28), where in the first terminal encrypts the payload of the broadcast frame using a broadcast encryption key of the first terminal (a private key is given in advance, col. 1, line 23), and the second terminal decodes the payload of the broadcast frame using the broadcast encryption key of the first terminal (the subscribers decode the received encrypted signals using the private key, which permits only those subscribers who have contracted for reception to watch and listen to the broadcast, col. 1, lines 25-29).

6. With respect to claim 2, Akachi discloses an encryption-key management list table having at least an encryption-key management list comprising a set of a terminal identifier of the first terminal and the broadcast encryption key of the first terminal (The device 113 includes an encryption key table storage unit 113A for storing an encryption key table in the form of a diagram oriented to the encryption key assigned to each MAC address, col. 13, lines 16-19); means for searching the encryption-key management list table based on the terminal identifier of the first terminal included in a start-terminal identifier of the received broadcast frame to extract the corresponding broadcast encryption key of the first terminal (When it is necessary to encrypt the data located in the payload, such as for an IP packet, the transmission processing device 113 retrieves an encryption key assigned to the MAC address of the terminal 124_i for arrangement within the section header. The encryption key is retrieved from the encryption key table stored in the encryption key table storage unit 113A and is used to encrypt an IP packet arranged in the payload of that section, col. 13, lines 36-44); and means for decoding the payload of the broadcast frame using the extracted broadcast encryption key of the

first terminal (the decoding unit 34 refers to a key table 37, using the MAC address of the information processing device 22, to obtain a decoding key from the key table 28. The decoding unit 34 then decodes the data stream D31 using the decoding key and supplies the resultant decoded data D34 to the checker 35, col. 6, lines 47-52).

7. With respect to claim 3, Akachi discloses a generated-key table that stores the broadcast encryption key of the first terminal (key table, fig. 2, element 37); means for encrypting the payload of the broadcast frame using the broadcast encryption key of the first terminal stored in the generated-key table (When it is necessary to encrypt the data located in the payload, such as for an IP packet, the transmission processing device 113 retrieves an encryption key assigned to the MAC address of the terminal 124_i for arrangement within the section header. The encryption key is retrieved from the encryption key table stored in the encryption key table storage unit 113A and is used to encrypt an IP packet arranged in the payload of that section, col. 13, lines 36-44); and means for transmitting the encrypted broadcast frame (A transmitter encrypts the broadcast data, using the private key, and transmits the data via a satellite. col. 1, lines 24-26).

8. With respect to claim 4, Akachi discloses a terminal comprising: an encryption-key management list table having at least one encryption-key management list comprising a set of a terminal identifier of a different terminal and a broadcast encryption key of the different terminal (key table, fig. 2, element 37); means for searching the encryption-key management list table for the encryption-key management list including a start-terminal identifier of a received broadcast frame to extract the

corresponding broadcast encryption key (wherein a table is searched to determine whether said read address indicates that said portion of said received data is intended for said group or is intended solely for said respective one of said plurality of processing devices, and when said portion of said received data is encrypted, said table is again searched to locate said stored address that coincides with said read address and then a decryption key corresponding to said stored address is retrieved, said decryption key being retrieved only when a stored value associated with said decryption key indicates that said decryption key is in a valid state, col. 22, lines 37-47); and means for decoding a payload of the broadcast frame using the extracted broadcast encryption key (When it is necessary to encrypt the data located in the payload, such as for an IP packet, the transmission processing device 113 retrieves an encryption key assigned to the MAC address of the terminal 124_i for arrangement within the section header. The encryption key is retrieved from the encryption key table stored in the encryption key table storage unit 113A and is used to encrypt an IP packet arranged in the payload of that section, col. 13, lines 36-44).

9. With respect to claim 5, Akachi discloses an encryption-key management list table having at least one encryption-key management list that stores a unicast encryption key between said terminal and a different terminal and a broadcast encryption key of the different terminal in association with a terminal identifier of the different terminal (key table, fig. 2, element 37and col. 13, lines 16-19); means for, when an end-terminal identifier of a received frame is a broadcast address, searching the encryption-key management list table for the encryption-key management list including

a start-terminal identifier of the frame to extract the corresponding broadcast encryption key as an encryption key, and when the end-terminal identifier of the received frame is other than a broadcast address, searching the encryption-key management list table for the encryption-key management list including a start-terminal identifier of the frame to extract the corresponding unicast encryption key as the encryption key (col. 22, lines 37-47); and means for decoding a payload of the frame using the extracted encryption key (col. 13, lines 36-44).

10. With respect to claim 6, Akachi discloses a generated-key table that stores a broadcast encryption key of said terminal (key table, fig. 2, element 37and col. 13, lines 16-19); means for encrypting a payload of a broadcast frame using the broadcast encryption key (col. 1, lines 24-25); and means for transmitting the encrypted broadcast frame (col. 1, lines 24-26).

11. With respect to claim 7, Akachi discloses a generated-key table that stores a broadcast encryption key of said terminal (key table, fig. 2, element 37and col. 13, lines 16-19); an encryption-key management list table having at least one encryption-key management list that stores a unicast encryption key between said terminal and a different terminal in association with a terminal identifier of the different terminal (The transmission processing device 13 stores an encryption key correspondence table which holds the Media Access Control (MAC) addresses, namely the identification numbers corresponding to the respective information processing devices 22, and which holds the private keys that correspond to each of the MAC addresses, col. 5, lines 58-63); means for, when a frame to be transmitted is a broadcast frame, encrypting a

payload of the broadcast frame using the broadcast encryption key of the generated-key table, and when the frame to be transmitted is a unicast frame, searching the encryption-key management list table for the encryption-key management list including an end-terminal identifier of the unicast frame to encrypt a payload of the unicast frame using the corresponding unicast encryption key (col. 22, lines 37-47); and means for transmitting the encrypted frame (col. 1, lines 24-26).

12. With respect to claim 8, Akachi discloses means for encrypting a terminal identifier and a broadcast encryption key of said terminal using a unicast encryption key of a transmission-destination terminal (a transmitter encrypts the broadcast data, col. 1, lines 24-25); and means for transmitting the encrypted terminal identifier and broadcast encryption key of said terminal to the transmission-destination terminal (A transmitter encrypts the broadcast data, using the private key, and transmits the data via a satellite. col. 1, lines 24-26).

13. With respect to claim 9, Akachi discloses an encryption-key management list table having at least one encryption-key management list that stores a broadcast encryption key of a different terminal in association with a terminal identifier of the different terminal (col. 5, lines 58-63); means for encrypting the encryption-key management list using a unicast encryption key of a transmission-destination terminal (encrypts the broadcast data, col. 1, lines 24-25); and means for transmitting the encrypted encryption-key management list to the transmission-destination terminal (col. 1, lines 24-26).

14. With respect to claim 10, Akachi discloses means for receiving a terminal identifier and a broadcast encryption key of a different terminal from the different terminal (fig. 7, element 107); means for encrypting the terminal identifier and the broadcast encryption key of the different terminal using a broadcast encryption key of said terminal (encrypts the broadcast data, col. 1, lines 24-25); and means for broadcasting the encrypted terminal identifier and broadcast encryption key of the different terminal (col. 1, lines 24-26).

15. With respect to claims 11and 15, Akachi discloses searching the encryption-key management list table for the encryption-key management list including a start-terminal identifier of a received broadcast frame to extract the corresponding broadcast encryption key (the decoding unit 34 searches the key table, line by line, using the expression (1), and determines whether a MAC address exists that coincides with the register MR of the key table, col. 10, lines 26-30); and decoding a payload of the broadcast frame using the extracted broadcast encryption key (the subscribers decode the received encrypted signals using the private key, which permits only those subscribers who have contracted for reception to watch and listen to the broadcast, col. 1, lines 25-29).

16. With respect to claims 12 and 16, Akachi discloses encrypting a payload of the broadcast frame using the broadcast encryption key stored in the generated-key table (a transmitter encrypts the broadcast data, col. 1, lines 24-25); and transmitting the encrypted broadcast frame (transmits the data, col. 1, lines 24-26).

17. With respect to claims 13 and 17, Akachi discloses receiving a terminal identifier and a broadcast encryption key of a first terminal that are encrypted using a unicast encryption key between the first terminal and the second terminal (fig. 7, element 107); decoding the encrypted terminal identifier and broadcast encryption key of the first terminal using the unicast encryption key (the subscribers decode the received encrypted signals using the private key, col. 1, lines 25-29); encrypting a terminal identifier and a broadcast encryption key of the second terminal using the unicast encryption key (encrypts the broadcast data, col. 1, lines 24-25); and transmitting the encrypted terminal identifier and broadcast encryption key of the second terminal to the first terminal (A transmitter encrypts the broadcast data, using the private key, and transmits the data via a satellite. col. 1, lines 24-26).

18. With respect to claims 14 and 18, Akachi discloses receiving a terminal identifier and a broadcast encryption key of a first terminal that are encrypted using a unicast encryption key between the first terminal and the second terminal (fig. 7, element 107); decoding the encrypted terminal identifier and broadcast encryption key of the first terminal using the unicast encryption key (the subscribers decode the received encrypted signals using the private key, col. 1, lines 25-29); encrypting the terminal identifier and the broadcast encryption key of the first terminal using a broadcast encryption key of the second terminal (encrypts the broadcast data, col. 1, lines 24-25); and transmitting the encrypted terminal identifier and broadcast encryption key of the first terminal to a third terminal (A transmitter encrypts the broadcast data, using the private key, and transmits the data via a satellite. col. 1, lines 24-26).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHAHROUZ YOUSEFI whose telephone number is (571) 270-3558. The examiner can normally be reached on Monday-Thursday 9:00-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 5712723799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. Y./
Examiner, Art Unit 2132
05/21/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132